SCOPE MANAGMENT PLAN

National Currency Printing and Secure Banknote Production Facility Project (NCPBF)

Project Title:

National Currency Printing and Secure Banknote Production Facility Project (NCPBF)

Project Sponsor:

Central Bank

Prepared by: PMIC of Lazuli Pamir Consulting – for learning purpose only

Table of Contents

1. Purpose of the Scope Management Plan:

The purpose of this Scope Management Plan is to establish a structured, disciplined, and governance-integrated framework for defining, managing, validating, and controlling the scope of the National Currency Printing and Secure Banknote Production Facility Project (NCPBF) throughout its entire lifecycle. Given the project's strategic national importance, high security sensitivity, multi-phase capital-intensive structure, and strict regulatory oversight environment, scope management is positioned not as a procedural formality, but as a critical governance control mechanism designed to protect project integrity, stability, and long-term value realization.

This plan defines how project scope will be clearly articulated, decomposed into manageable deliverables, formally approved through authorized governance bodies, validated at defined milestone points, monitored throughout execution, and protected from uncontrolled or informal modification. By establishing these controls, the plan ensures that the project delivers precisely the outputs and capabilities approved in the Business Case and Project Charter, while maintaining alignment with strategic objectives, financial constraints, security requirements, and regulatory obligations.

In complex national infrastructure projects such as NCPBF, scope instability is one of the most significant threats to successful delivery. Uncontrolled enhancements, politically motivated additions, vendor-driven specification expansions, or informal executive requests can introduce cascading impacts on schedule, cost, risk exposure, security architecture, and operational readiness. This Scope Management Plan creates formal boundaries that prevent such disruptions. It ensures that any proposed modification to the approved baseline undergoes structured impact analysis, documented justification, and appropriate governance review before authorization. Through this disciplined approach, the project avoids scope drift, protects approved investment assumptions, and preserves delivery predictability.

The plan also ensures strong strategic alignment. The NCPBF project exists to establish a secure, sovereign, and sustainable national banknote production capability that strengthens monetary integrity and institutional resilience. Every defined deliverable must directly contribute to this strategic intent. Scope elements

that do not demonstrate traceability to approved business objectives, measurable benefits, or defined operational capabilities are subject to challenge and review. By enforcing this alignment, the Scope Management Plan safeguards the long-term value proposition articulated in the Business Case and ensures that execution remains focused on intended national outcomes rather than peripheral or non-essential enhancements.

Financial discipline is another central purpose of this plan. Scope growth is a primary driver of cost overruns in large infrastructure initiatives. This Scope Management Plan ensures that the approved scope baseline remains tightly integrated with the cost baseline and funding approvals. No additional deliverables may be initiated without formal change authorization and corresponding budget validation. Proposed scope changes must include comprehensive cost impact analysis, funding source identification, and reserve evaluation before consideration. This integration between scope control and financial governance preserves investment viability and protects the economic assumptions underpinning the project's feasibility analysis.

Security integrity is equally fundamental to the purpose of this plan. The NCPBF project involves secure printing technologies, cybersecurity systems, restricted infrastructure components, access control mechanisms, and confidential regulatory frameworks. Modifications to scope in such environments carry not only financial or schedule implications, but also potential security vulnerabilities. The Scope Management Plan ensures that security-sensitive deliverables cannot be altered without appropriate review by authorized security governance bodies. It embeds security impact assessment into change evaluation processes and enforces strict configuration control for classified components. Through this mechanism, the project maintains a security-by-design posture throughout execution and commissioning.

Regulatory compliance and audit transparency further reinforce the importance of disciplined scope control. The project must adhere to national currency regulations, procurement frameworks, institutional governance policies, and oversight requirements. This plan ensures that scope remains compliant by requiring regulatory impact evaluation for any proposed change and maintaining documented traceability between approved requirements and executed deliverables. By preserving structured documentation, version control, and formal

approval records, the project maintains audit readiness and institutional accountability.

The Scope Management Plan also protects benefits realization integrity. The ultimate success of the NCPBF project is not measured solely by physical completion of a facility, but by realization of long-term operational, financial, security, and institutional benefits. Uncontrolled scope expansion or misalignment can dilute focus, delay commissioning, increase complexity, or compromise the capability required to achieve intended outcomes. This plan ensures that every deliverable supports measurable benefits defined in the Benefits Management Plan and that scope changes are evaluated against their impact on long-term value creation. Through this discipline, the project bridges the gap between output delivery and sustainable operational impact.

Furthermore, this plan reinforces governance discipline by clearly defining authority boundaries and escalation pathways. Scope decisions are not made informally or through unilateral instruction. Instead, they are reviewed within structured decision frameworks defined by the Project Governance Framework. Depending on impact magnitude, changes may require review by the Change Control Board, Steering Committee, or Project Sponsor. This formal decision architecture prevents bypassing of controls, reduces ambiguity, and ensures accountability in scope-related decisions.

Continuous monitoring of scope performance is also embedded within the purpose of this plan. Change frequency trends, variance analysis, deliverable completion stability, and stage-gate validation outcomes are reviewed to detect early signs of scope instability. Where excessive change patterns emerge, governance review is triggered to assess root causes and implement corrective measures. This proactive monitoring ensures that scope remains controlled and predictable rather than reactive and unstable.

In summary, the purpose of this Scope Management Plan is to safeguard the NCPBF project from uncontrolled expansion, strategic deviation, financial erosion, security exposure, and governance breakdown. It establishes a disciplined environment in which scope is clearly defined, formally authorized, transparently monitored, and rigorously protected. Through structured definition, decomposition, validation, control, and monitoring mechanisms, the project ensures that execution remains

aligned with approved objectives and that the intended national capability is delivered with integrity, accountability, and long-term sustainability.

Scope management within the NCPBF context is therefore not merely a planning activity; it is a strategic safeguard that protects national investment, institutional credibility, operational readiness, and enduring value realization.

2. Scope Management Objectives:

The Scope Management Plan establishes a set of clear and disciplined objectives designed to ensure that the National Currency Printing and Secure Banknote Production Facility Project (NCPBF) delivers exactly what has been formally authorized—no more and no less. Given the project's strategic national importance, financial scale, security sensitivity, and multi-layered governance environment, scope management objectives must extend beyond simple deliverable definition and focus on strategic alignment, control integrity, and long-term value protection.

A primary objective of this plan is to ensure full and continuous alignment with the approved Business Case. The Business Case defines the strategic justification, investment rationale, selected solution option, expected benefits, financial feasibility, and national objectives of the project. Scope must remain fully consistent with those foundational assumptions. Any deviation from the defined solution architecture or capability design must be evaluated against the Business Case to confirm continued strategic validity. This objective ensures that the project does not gradually drift away from its original investment intent through incremental or uncoordinated changes.

Another critical objective is the protection of the formally approved scope baseline defined in the Scope Statement. The baseline represents the authoritative reference point against which all performance measurement, change evaluation, and governance review are conducted. Preserving this baseline is essential for maintaining schedule stability, cost predictability, risk discipline, and governance credibility. The Scope Management Plan therefore aims to prevent unauthorized work, informal enhancements, undocumented modifications, or unapproved commitments that could undermine baseline integrity. Stability of the baseline is treated as a performance indicator in itself.

The plan also seeks to establish and maintain full traceability across the project's documentation ecosystem. In a project of this complexity, traceability is essential to maintain transparency and governance discipline. The Scope Management Plan ensures structured linkage between the Business Case, Project Charter, Scope Statement, Work Breakdown Structure (WBS), defined deliverables, and the Benefits Management Plan. This end-to-end traceability ensures that each work package exists for a justified strategic reason and contributes to measurable outcomes. It

also supports audit readiness and provides clarity in impact analysis when scope modifications are proposed.

Integration with other management systems is another central objective. Scope control cannot operate in isolation; it must function as part of a coordinated governance architecture. The Scope Management Plan is therefore designed to operate in direct alignment with the Risk Management Plan, ensuring that proposed changes trigger risk reassessment and mitigation updates. It is integrated with the Assumption Log, recognizing that invalidated assumptions may necessitate controlled scope adjustments. It connects with the Issue Log, ensuring that emerging issues are addressed without bypassing formal scope control mechanisms. It is also embedded within the Project Governance Framework, ensuring that scope decisions respect defined authority levels and escalation thresholds. This integration ensures consistency, prevents fragmented decision-making, and reinforces structured accountability.

A further objective of this plan is the enforcement of stage-gate approval discipline. The NCPBF project operates under a phased lifecycle model, where transitions between major execution stages—such as design finalization, construction commencement, system installation, and commissioning—require formal validation and approval. The Scope Management Plan ensures that no phase transition occurs without confirmation that the defined scope for that stage has been fully validated, accepted, and frozen. This prevents rework, premature progression, and late-stage design alterations that could destabilize execution.

Given the project's national-level security sensitivity, protecting security-related deliverables from informal modification is a key objective. Certain components of the project—such as secure printing systems, cybersecurity architecture, access control mechanisms, vault systems, and surveillance infrastructure—are security-critical. Changes to these elements may introduce vulnerabilities or compromise regulatory compliance. The Scope Management Plan therefore establishes strict controls requiring that security-sensitive deliverables undergo enhanced review by authorized governance bodies before any modification is approved. This ensures that scope flexibility does not undermine security integrity.

Another essential objective is ensuring that all proposed scope changes undergo structured and documented impact analysis prior to approval. Change analysis

must consider implications across schedule, cost, risk exposure, regulatory compliance, security architecture, operational readiness, and benefits realization. No modification may be authorized based solely on perceived operational advantage or stakeholder preference. Instead, structured evaluation ensures that decision-makers fully understand downstream consequences. This protects the project from reactive or short-term decisions that could create long-term instability.

Additionally, the Scope Management Plan aims to preserve financial discipline and cost containment. Scope growth is a primary driver of budget overruns in complex infrastructure initiatives. By requiring formal cost impact analysis and governance approval for any scope modification, the plan ensures that financial feasibility remains intact and that contingency reserves are not eroded without deliberate decision-making.

The plan also seeks to maintain predictability and execution stability. Excessive scope change frequency often indicates governance weakness or stakeholder misalignment. By monitoring change trends and escalation patterns, the Scope Management Plan contributes to early detection of instability and supports corrective governance intervention where necessary.

Ultimately, the objectives of this Scope Management Plan converge toward a single overarching principle: disciplined delivery of authorized capability within approved boundaries. Through alignment with strategic intent, protection of the baseline, structured traceability, integration with risk and governance systems, enforcement of stage-gate discipline, safeguarding of security-sensitive elements, and mandatory impact analysis for all changes, the project preserves its integrity and maximizes its probability of successful, secure, and sustainable completion.

3. Scope Definition Approach:

3.1 Authoritative Inputs:

The definition of scope for the National Currency Printing and Secure Banknote Production Facility Project (NCPBF) is derived exclusively from formally approved and governance-controlled documents. Scope is not developed through informal requirement gathering or isolated technical interpretation; rather, it is systematically constructed from strategic, legal, and governance-authorized sources to ensure alignment, legitimacy, and traceability.

The primary authoritative input into scope definition is the approved Business Case. The Business Case establishes the strategic rationale for investment, defines the selected solution option, outlines expected capabilities, articulates measurable benefits, and confirms financial feasibility. All scope elements must directly support the selected investment option and deliver the capabilities justified within that document. Any deliverable that cannot demonstrate alignment with the Business Case requires formal justification and approval.

The Project Charter serves as the formal authorization instrument that translates strategic intent into defined project objectives, high-level deliverables, authority boundaries, and success criteria. Scope must remain consistent with the Charter's mandate. The Charter defines what the project is authorized to deliver and establishes the limits within which execution must occur. No work may be initiated beyond these authorized boundaries without structured governance review.

The Governance Framework provides the structural mechanism through which scope authority is exercised and controlled. It defines decision rights, approval thresholds, stage-gate requirements, and escalation pathways. Scope definition is therefore embedded within governance discipline. Authority to approve or modify scope resides only within formally designated governance bodies, ensuring transparency, accountability, and protection against informal or unilateral scope expansion.

The Project Vision Statement contributes a long-term institutional perspective to scope definition. While the Business Case defines financial and strategic justification, the Vision Statement articulates the desired future state of sovereign, secure, and sustainable national banknote production capability. Scope must

therefore reflect not only physical construction and technical installation, but also capability development, sustainability, and governance maturity elements necessary to achieve that vision.

The High-Level Roadmap informs scope by defining lifecycle phases, sequencing logic, milestone structure, and transitional dependencies. Scope definition must be aligned with phased execution to prevent premature, fragmented, or improperly sequenced deliverables. Each major scope component is positioned within a lifecycle phase to ensure orderly progression from authorization through commissioning and operational transition.

Regulatory and compliance requirements represent mandatory inputs into scope definition. Currency production and secure facility development are subject to national monetary regulations, procurement laws, audit standards, and security frameworks. Scope must therefore incorporate all compliance-driven deliverables as integral components rather than optional enhancements. Failure to embed regulatory requirements within defined scope would create exposure to legal, financial, and reputational risk.

Based on these authoritative inputs, scope is formally defined, documented, and approved. No scope element may be added, modified, or removed without formal change control approval in accordance with the established governance structure. This ensures disciplined boundary management and preserves the integrity of the approved baseline.

3.2 Scope Categories:

To ensure clarity, governance visibility, and lifecycle control, the NCPBF scope is organized into structured and controlled categories representing the complete capability architecture required to establish a secure national banknote production facility. These categories reflect both physical infrastructure components and institutional capability elements necessary for sustainable and secure operation.

The scope is structured under the following controlled categories:

1. Facility Infrastructure Construction

This category includes all physical works required to establish the secure production environment. It encompasses site preparation, structural construction,

vault systems, controlled access zones, perimeter security infrastructure, environmental control systems, utilities, and supporting facilities. These deliverables form the foundational backbone upon which all technical systems and operational capabilities depend. Infrastructure scope must meet structural, environmental, and security specifications defined in regulatory and governance requirements.

2. Secure Printing Systems & Technology

This category includes procurement, installation, calibration, integration, and validation of specialized banknote printing machinery and related technologies. It covers printing presses, inspection systems, finishing equipment, material handling systems, and embedded quality control mechanisms. Due to the sensitivity and technical complexity of these systems, this scope domain requires strict configuration control, vendor coordination, and performance validation before acceptance.

3. Cybersecurity & Security Controls

This category addresses digital and physical security architecture. It includes secure network infrastructure, access control systems, surveillance and monitoring systems, intrusion detection mechanisms, data protection frameworks, and secure communications platforms. Given the national-level sensitivity of currency production, this category is subject to enhanced review and security governance oversight to ensure confidentiality, integrity, and operational resilience.

4. Operational Readiness & Training

This category ensures that the facility is capable of sustained and compliant operation upon completion. It includes development of standard operating procedures, structured staff training programs, knowledge transfer from technology vendors, competency validation, operational simulations, and readiness assessments. Deliverables within this category transform installed infrastructure and systems into functional institutional capability.

5. Governance & Compliance Systems

This category includes establishment of oversight mechanisms, reporting structures, segregation-of-duties controls, documentation systems, regulatory compliance processes, and audit frameworks. These deliverables ensure that the

facility operates under disciplined governance and remains compliant with national monetary regulations, security frameworks, and institutional policies.

6. Commissioning & Certification

This category includes all validation and approval processes required prior to operational activation. It encompasses factory acceptance testing (FAT), site acceptance testing (SAT), integrated system validation, performance testing, security certification, regulatory confirmation, and formal readiness approval. Commissioning ensures that all defined deliverables meet established performance, quality, and security standards before handover.

7. Transition to Operations

This final category includes formal asset handover, operational governance activation, documentation transfer, performance baseline establishment, and initiation of benefits tracking. It ensures continuity between project execution and steady-state operational ownership, protecting long-term sustainability and value realization.

All of the above categories are fully decomposed within the approved Work Breakdown Structure (WBS) and elaborated at work-package level within the WBS Dictionary. Each work package contains defined deliverables, acceptance criteria, assigned ownership, and dependency mapping. Scope is therefore controlled not only at category level but also at detailed work-package level, ensuring measurable accountability and governance oversight.

Through this structured categorization, the project achieves clarity of boundaries, lifecycle alignment, and disciplined scope governance, preventing uncontrolled expansion and ensuring delivery of authorized national capability.

4. Work Breakdown Structure (WBS) Integration:

Scope decomposition within the National Currency Printing and Secure Banknote Production Facility Project (NCPBF) follows a structured, deliverable-based approach to ensure clarity, traceability, governance alignment, and control integrity. The Work Breakdown Structure (WBS) serves as the formal architecture through which approved scope is decomposed into manageable, measurable, and governable components.

The WBS is not a schedule, task list, or activity register. It is a hierarchical representation of the total authorized project scope, organized around tangible deliverables rather than actions. In this project, deliverables define scope; activities are only the means of producing those deliverables and therefore are not considered scope elements.

The WBS is structured across three primary levels:

Level 1 – NCPBF Project:

This level represents the entire authorized project scope as approved in the Project Charter and Scope Statement. It reflects the full capability required to establish and operationalize the secure banknote production facility.

Level 2 – Control Accounts (Major Deliverable Streams):

At this level, the total project scope is divided into major deliverable categories aligned with the approved Scope Categories, such as Infrastructure Construction, Secure Printing Systems, Cybersecurity Controls, Operational Readiness, Governance Systems, Commissioning, and Transition to Operations. These control accounts represent management-level scope components and serve as primary reporting and monitoring units.

Level 3 – Work Packages:

Work packages represent the lowest level of scope decomposition within the WBS. Each work package defines a clearly measurable and verifiable deliverable. Work packages must be sufficiently detailed to allow cost estimation, resource assignment, performance measurement, and governance control, while avoiding unnecessary fragmentation that could complicate oversight.

Every work package included in the WBS must comply with the following guidelines:

- It must represent a deliverable outcome, not an activity.
- It must have clearly defined acceptance criteria.
- It must be measurable and verifiable.
- It must be assigned to a responsible owner.
- It must be traceable to higher-level objectives.
- It must fall entirely within approved scope boundaries.

To ensure governance strength and traceability, each work package defined in the WBS is further elaborated in the WBS Dictionary.

The WBS Dictionary is the authoritative reference document that provides detailed definitions and control information for each work package. It supplements the hierarchical WBS by describing what each deliverable includes and excludes, how it will be validated, and who is accountable for its completion.

For each work package, the WBS Dictionary must include:

- Work Package Title and Unique Identifier
- Detailed Description of Deliverable Scope
- Key Deliverables and Outputs
- Explicit Inclusions and Exclusions
- Acceptance Criteria and Quality Requirements
- Assigned Ownership and Accountability
- Dependencies and Interfaces
- Linked Risk References
- Linked Benefit References
- Stage-Gate Validation Requirements

This structured documentation ensures that scope is not ambiguously interpreted and that all stakeholders share a common understanding of deliverable boundaries.

Integration between the WBS and WBS Dictionary ensures that scope is fully traceable and governable. Every element in the WBS must have a corresponding entry in the WBS Dictionary, and no work may be initiated unless it is represented within the approved WBS structure.

Additionally, each work package must be formally integrated with other project control systems. Specifically:

- Work packages must be linked to identified risks within the Risk Register to ensure proactive risk management.
- Where applicable, work packages must be linked to measurable benefits defined in the Benefits Management Plan to preserve strategic alignment.
- Ownership assignments must align with the Resource Management Plan to ensure accountability.
- Validation checkpoints must align with stage-gate reviews defined in the Governance Framework.

The WBS also supports financial and schedule integration. Cost estimation, budget allocation, and performance measurement (including Earned Value analysis where applicable) are structured around WBS control accounts and work packages. This ensures that cost, schedule, and scope remain aligned and measurable within a unified governance framework.

Changes to scope are managed through controlled modification of the WBS and corresponding updates to the WBS Dictionary. No work package may be added, removed, or modified without formal change control approval. Approved changes must trigger updates to:

- WBS structure
- WBS Dictionary entries
- Risk references
- Cost baseline
- Schedule baseline
- Benefits traceability documentation

This disciplined integration ensures that the WBS functions not merely as a planning artifact, but as the central structural mechanism through which scope integrity is preserved.

In summary, the Work Breakdown Structure and its supporting WBS Dictionary form the backbone of scope governance within the NCPBF project. They transform high-level strategic intent into controlled, measurable, and accountable deliverables. By

enforcing a deliverable-based decomposition approach and integrating each work package with risk, benefits, ownership, and stage-gate oversight, the project ensures that scope remains stable, transparent, and aligned with approved objectives.

Activities do not define scope. Deliverables define scope. The WBS defines those deliverables. The WBS Dictionary governs them.

---

5. Scope Baseline Components:

The Scope Baseline consists of:

1. Approved Scope Statement
2. Approved WBS
3. Approved WBS Dictionary

The Scope Baseline represents the formally approved version of the project scope against which scope performance is measured and controlled. It establishes the official reference point for determining whether deliverables are within approved boundaries and for evaluating the impact of proposed changes.

In accordance with PMI standards, the Scope Baseline for the NCPBF Project consists of the following three integrated components:

5.1 Project Scope Statement:

The Project Scope Statement provides a detailed description of the project scope, including:

- Product scope description
- Project deliverables
- Acceptance criteria
- Project exclusions
- Constraints and assumptions related to scope

This document defines what is included and explicitly clarifies what is excluded from the project. It translates high-level objectives from the Project Charter into a comprehensive and structured scope definition. The Scope Statement establishes boundary clarity and prevents ambiguity in interpretation of deliverables.

5.2 Work Breakdown Structure (WBS):

The Work Breakdown Structure decomposes the total approved project scope into hierarchical deliverable components. It organizes scope into progressively smaller and more manageable elements, ensuring completeness and structural clarity.

The WBS:

- Represents 100% of the approved project scope (100% Rule)
- Is deliverable-oriented, not activity-based

- Provides the structural framework for cost and schedule integration
- Serves as the foundation for performance measurement

The WBS defines what must be delivered but does not describe how the work will be performed.

5.3 WBS Dictionary:

The WBS Dictionary complements the WBS by providing detailed descriptions of each work package. It ensures consistent interpretation of scope and prevents misalignment across stakeholders.

For each work package, the WBS Dictionary includes:

- Detailed scope description
- Deliverable definition
- Acceptance criteria
- Responsible owner
- Boundaries (inclusions and exclusions)
- Dependencies and interfaces
- Relevant constraints

Together, the WBS and WBS Dictionary eliminate ambiguity and ensure that deliverables are clearly defined and verifiable.

5.4 Scope Baseline Control and Configuration Management:

Once approved, the Scope Baseline becomes part of the integrated project management baseline and is subject to formal configuration control.

Configuration management ensures that:

- The baseline version is formally documented and stored
- Changes are traceable and version-controlled
- Unauthorized modifications are prevented
- Historical baseline records are preserved

Any change to the Scope Baseline — including modifications to the Scope Statement, WBS structure, or WBS Dictionary definitions — requires formal change control approval in accordance with the project's governance framework.

No work may be initiated that is not represented within the approved Scope Baseline.
No baseline component may be modified without documented impact analysis and authorized approval.

Approved changes must result in:

- Updated Scope Statement (if applicable)
- Updated WBS and WBS Dictionary
- Corresponding updates to cost and schedule baselines
- Re-alignment of risk and benefits documentation

Through disciplined configuration management and structured change governance, the Scope Baseline ensures that scope integrity, financial control, and strategic alignment are preserved throughout the lifecycle of the NCPBF project.

6. Scope Validation Process:

Scope validation is the formal process of obtaining stakeholder acceptance of completed deliverables. In alignment with PMI standards, scope validation focuses on verifying that completed deliverables meet the approved scope and documented acceptance criteria defined in the Scope Baseline (Scope Statement, WBS, and WBS Dictionary).

Within the NCPBF Project, scope validation is treated as a structured governance activity integrated with stage-gate reviews and lifecycle control mechanisms. It ensures that deliverables are formally reviewed, verified, and accepted before progression to subsequent phases.

Scope validation occurs at defined lifecycle checkpoints, including but not limited to:

- Design approval stage
- Construction milestone completion
- Equipment installation completion
- Security certification review
- Operational readiness review
- Final commissioning

These validation points are aligned with the High-Level Roadmap and Governance Framework to ensure structured phase transitions and prevent premature advancement.

6.1 Validation Criteria:

Each deliverable must be validated against pre-defined acceptance criteria documented in the WBS Dictionary and Scope Statement. Acceptance criteria must be:

- Measurable
- Objective
- Verifiable
- Aligned with regulatory and security requirements

Validation confirms that the deliverable satisfies scope requirements and complies with defined performance, quality, security, and regulatory standards.

6.2 Validation Activities:

Scope validation includes the following structured activities:

- Deliverable inspection to confirm completion and conformity
- Verification of compliance with technical specifications
- Regulatory and standards compliance confirmation
- Security clearance confirmation for classified components
- Review against defined acceptance criteria
- Documentation of inspection results
- Formal stakeholder review and approval

Inspection methods may include physical verification, document review, testing reports, certification records, audit confirmation, or integrated system validation results depending on the nature of the deliverable.

6.3 Roles and Responsibilities:

The Project Manager coordinates the validation process and ensures that deliverables are presented for formal acceptance only after internal quality control confirmation.

Designated reviewers may include:

- Technical authorities
- Compliance officers
- Security governance representatives
- Operational readiness assessors
- Steering Committee representatives
- Project Sponsor (where required)

Final acceptance authority rests with the authorized governance body or Sponsor, depending on deliverable criticality and approval thresholds defined in the Governance Framework.

6.4 Documentation of Acceptance:

No deliverable is considered complete until documented acceptance has been obtained. Acceptance documentation must include:

- Description of the validated deliverable
- Reference to applicable WBS work package

- Confirmation of compliance with acceptance criteria
- Date of validation
- Authorized sign-off

Accepted deliverables are formally recorded and archived under configuration control. Rejected deliverables must undergo corrective action prior to re-submission for validation.

6.5 Relationship Between Validate Scope and Quality Control:

In accordance with PMI guidance, quality control (Control Quality process) precedes scope validation. Control Quality verifies that deliverables meet defined quality requirements, while Validate Scope formally obtains stakeholder acceptance.

A deliverable that fails quality control cannot proceed to validation. This separation ensures that stakeholder review focuses on scope conformity rather than defect correction.

6.6 Governance Integration:

Scope validation results are reported to governance bodies at defined stage-gate checkpoints. Phase transitions cannot proceed without formal confirmation that all required deliverables for that stage have been validated and accepted.

Failure to achieve validation triggers issue logging, corrective action planning, and possible schedule adjustment under integrated change control procedures.

6.7 Completion Definition:

For the NCPBF project, a deliverable is considered complete only when:

- It has been produced in accordance with the approved Scope Baseline
- It has passed quality verification
- It meets documented acceptance criteria
- It complies with security and regulatory requirements
- It has received formal documented acceptance

Completion without documented acceptance is not recognized as valid progress.

7. Scope Control Process:

The Scope Control Process ensures that the Scope Baseline remains stable, traceable, and aligned with approved strategic intent throughout the lifecycle of the NCPBF Project. In accordance with PMI's Perform Integrated Change Control process, no modification to the approved scope may be implemented without structured evaluation, documented authorization, and formal baseline adjustment. Scope control protects the project from uncontrolled expansion, informal commitments, cost escalation, security exposure, and strategic misalignment.

All scope changes must follow the structured process defined below.

Step 1: Change Identification

The scope control process begins when a potential change to approved scope is formally identified. A change may originate from technical discoveries, regulatory updates, stakeholder requests, security findings, risk responses, operational readiness gaps, or governance recommendations.

No scope modification may proceed informally through verbal agreement, email confirmation, or executive instruction. Every proposed change must be formally documented and logged in the Change Register. The change entry must clearly describe:

- The requested modification
- The reason for the change
- The affected deliverables or WBS elements
- The originator of the request
- The urgency and classification level

Formal logging ensures transparency, traceability, and accountability. It prevents unauthorized work initiation and provides an auditable record of all proposed scope adjustments.

Step 2: Impact Analysis

Once a change request is logged, a structured impact analysis is conducted. The objective of this step is to ensure that decision-makers understand the full consequences of the proposed modification before approval is granted.

The impact analysis must comprehensively evaluate:

- **Schedule impact**, including milestone shifts, stage-gate delays, and critical path effects.
- **Cost impact**, including direct expenses, indirect overhead implications, contingency usage, and funding source availability.
- **Security implications**, particularly for classified systems, secure infrastructure, cybersecurity architecture, and access controls.
- **Regulatory impact**, ensuring continued compliance with monetary, procurement, and audit frameworks.
- **Risk exposure**, including introduction of new risks, modification of existing risk ratings, or mitigation strategy adjustments.
- **Benefits alignment**, confirming that the proposed change supports or enhances intended long-term value realization.

The analysis must be evidence-based and documented. No decision may be made without a structured evaluation across these impact dimensions. This prevents short-term convenience decisions that could generate long-term instability.

Step 3: Risk and Assumption Review

Following impact analysis, all related risks and assumptions must be reassessed. Scope changes frequently alter project uncertainty levels, invalidate prior assumptions, or introduce new exposure areas.

The Risk Register must be reviewed to determine whether:

- Existing risks require re-rating
- New risks must be logged
- Mitigation or contingency strategies require revision
- Risk reserves must be adjusted

Similarly, assumptions recorded in the Assumption Log must be evaluated to determine whether the proposed change confirms, modifies, or invalidates underlying assumptions.

This step ensures that scope control remains integrated with risk management and prevents unintended consequences arising from unassessed uncertainty shifts.

Step 4: Governance Review

After technical and risk analysis is completed, the change request proceeds to formal governance review. The level of escalation depends on defined authority thresholds within the Governance Framework.

Escalation criteria typically include:

- Cost magnitude relative to approved thresholds
- Impact on stage-gate commitments
- Security classification sensitivity
- Strategic alignment implications
- Regulatory exposure

Minor changes within predefined tolerance levels may be reviewed by the Change Control Board (CCB). Significant changes affecting strategic objectives, funding allocations, or security architecture may require Steering Committee or Project Sponsor approval.

This governance layer ensures that authority is exercised appropriately and that scope changes reflect institutional decision-making rather than operational convenience.

Step 5: Decision

Following governance review, a formal decision is issued. The decision must be documented and communicated to relevant stakeholders.

The decision may result in:

- **Approval**, authorizing implementation of the change.
- **Rejection**, denying the modification and preserving baseline integrity.
- **Deferral**, postponing decision pending additional analysis or future review.

No work related to the proposed change may begin until formal approval is documented. Unauthorized implementation of rejected or unapproved changes constitutes a governance violation and may trigger corrective action.

Step 6: Baseline Update

If the change is approved, the Scope Baseline and all affected project management components must be formally updated under configuration management control.

This includes updating:

- The **Scope Statement**, if the scope definition is modified.
- The **WBS and WBS Dictionary**, to reflect structural or deliverable changes.
- The **Cost Baseline and Budget Documentation**, if financial adjustments are required.
- The **Schedule Baseline**, if milestone dates are impacted.
- The **Risk Register**, incorporating updated exposure and mitigation measures.
- The **Benefits Tracking Documentation**, if strategic value realization is affected.

All updates must be version-controlled, documented, and communicated to relevant stakeholders. The revised baseline becomes the new performance reference for ongoing monitoring and reporting.

Failure to formally update baselines following approval creates misalignment between execution and governance documentation and is therefore prohibited.

Scope Control Integrity Principle

The NCPBF project operates under a strict principle: no scope change without documented impact analysis, governance authorization, and baseline update.

Through this structured six-step process, scope control becomes an integrated governance mechanism that protects strategic alignment, financial sustainability, regulatory compliance, security integrity, and long-term benefit realization.

Scope stability is not rigidity; it is disciplined flexibility exercised under formal authority.

8. Governance Integration:

Effective scope management within the NCPBF Project is inseparable from its governance architecture. Given the project's national significance, security sensitivity, financial scale, and regulatory exposure, scope control decisions are not treated as operational adjustments but as governance matters. All scope modifications are reviewed, evaluated, and authorized within formally established decision-making bodies to ensure accountability, transparency, and strategic discipline.

Scope changes are reviewed at defined governance levels depending on their magnitude, impact, and classification.

8.1 Change Control Board (CCB):

The Change Control Board serves as the primary governance body responsible for reviewing and deciding upon scope changes that fall within predefined tolerance thresholds. The CCB evaluates change requests after completion of structured impact analysis and risk assessment.

The Board reviews:

- Scope alignment with approved objectives
- Cost and schedule implications
- Risk exposure adjustments
- Technical feasibility
- Resource availability
- Compliance implications

Changes that do not materially affect strategic objectives, approved funding envelopes, or security architecture may be authorized at the CCB level. The CCB ensures that minor or moderate adjustments are handled efficiently while preserving baseline integrity.

All CCB decisions are formally documented and archived under configuration management procedures.

8.2 Steering Committee Review (High-Impact Changes):

Scope changes that exceed predefined cost thresholds, materially affect timeline commitments, alter major deliverable streams, or introduce significant risk exposure must be escalated to the Steering Committee.

The Steering Committee provides oversight for high-impact changes and ensures that modifications remain aligned with institutional priorities and governance principles. At this level, decisions consider:

- Long-term strategic implications
- Budget reallocation consequences
- Stakeholder alignment
- Regulatory exposure
- Interdependencies across workstreams

The Steering Committee ensures that major scope adjustments are not approved solely on operational justification but are evaluated from a broader institutional and governance perspective.

8.3 Executive Sponsor Approval (Strategic Deviation):

Changes that materially alter the original investment intent, redefine core project objectives, impact national security architecture, or significantly modify expected benefits require review and authorization by the Executive Sponsor.

Executive Sponsor involvement is mandatory when:

- The strategic direction of the project is affected
- Core capability objectives are modified
- Financial viability assumptions change
- Security or regulatory posture is materially impacted

This level of review ensures that deviations from the approved Business Case receive the highest level of institutional scrutiny and authorization.

No strategic deviation may be implemented without explicit Sponsor approval.

8.4 Stage-Gate Integration and Scope Freeze Discipline:

In addition to change governance bodies, scope management is reinforced through structured stage-gate reviews aligned with the project lifecycle. These

gates ensure disciplined progression between major execution phases and protect the project from late-stage instability.

Stage-gate reviews enforce scope freeze requirements at critical transition points, including:

- Scope freeze prior to commencement of construction activities
- Scope freeze prior to procurement of specialized equipment
- Scope freeze prior to commissioning and certification

Scope freeze means that the defined deliverables for that phase are formally validated, approved, and locked before downstream commitments are made. This prevents costly redesign, contract modification, rework, and regulatory exposure.

For example, construction may not begin until design scope has been validated and frozen. Similarly, equipment procurement may not proceed until technical specifications are formally approved and protected from modification. Prior to commissioning, integration scope must be fully confirmed to avoid operational delays.

Any exception to scope freeze requires formal governance review and documented justification.

8.5 Governance Transparency and Documentation:

All governance decisions related to scope changes must be:

- Documented in official records
- Linked to change request identifiers
- Version-controlled
- Communicated to affected stakeholders

This ensures audit readiness, institutional transparency, and accountability for decision outcomes.

9. Scope & Risk Integration:

In a project of the scale, complexity, and national sensitivity of the NCPBF initiative, scope management cannot operate independently of risk management. Every modification to approved scope has the potential to alter the project's risk profile, introduce new uncertainties, invalidate prior assumptions, or modify exposure levels across technical, financial, regulatory, and security domains. Therefore, scope control and risk management are formally integrated to ensure disciplined decision-making and institutional protection.

For every proposed scope change, risk exposure must be reassessed in a structured and documented manner. This reassessment ensures that decision-makers understand how the modification affects existing risk ratings, probability levels, impact severity, mitigation strategies, and overall risk posture. Even seemingly minor changes may create cascading effects in complex environments such as secure facility construction, cybersecurity architecture, or specialized equipment integration.

The first step in scope–risk integration is the systematic review of the Risk Register. When a change request is submitted, the project team evaluates whether the proposed modification affects any currently identified risks. Existing risks may require re-scoring due to altered technical conditions, new vendor dependencies, schedule compression, or expanded scope boundaries. A change that accelerates installation activities, for example, may increase integration risk or quality risk. A modification to infrastructure design may alter security risk exposure or regulatory compliance risk.

In addition to reassessing existing risks, the process requires identification of new risks introduced by the proposed change. Scope expansion often introduces new technical interfaces, contractual obligations, stakeholder dependencies, cybersecurity considerations, or regulatory implications. These must be formally identified, analyzed, categorized, and recorded in the Risk Register prior to approval. Failure to identify newly introduced risks may result in unmanaged exposure and reactive crisis management during execution.

Mitigation plans must also be updated to reflect the revised risk landscape. If a change increases exposure in certain areas, corresponding preventive or corrective actions must be defined before implementation. This ensures that risk

response strategies evolve proportionately with scope adjustments. Mitigation planning may include additional testing, revised sequencing, enhanced security reviews, or strengthened oversight mechanisms.

Contingency reserves represent another critical dimension of scope–risk integration. Scope modifications frequently alter the project's contingency requirements. An expansion of technical scope may increase cost risk and therefore require adjustment of management reserves. Similarly, schedule-related scope adjustments may affect time contingency allocations. Before approval, the project must evaluate whether existing contingency reserves remain adequate or require adjustment. Approval of scope changes without corresponding reserve evaluation undermines financial discipline and may compromise budget stability.

Integration with the Assumption Log is also essential. Scope changes may confirm, modify, or invalidate existing assumptions related to vendor performance, regulatory interpretation, resource availability, or technical feasibility. When assumptions shift, associated risk levels may increase. Therefore, assumption reassessment forms part of the integrated scope–risk evaluation.

Importantly, no scope expansion may be approved without documented risk assessment. This principle is non-negotiable within the NCPBF governance model. Informal or expedited approvals without risk evaluation expose the project to unmanaged uncertainty and compromise institutional accountability. Scope expansion without structured risk analysis is strictly prohibited.

The integration between scope and risk ensures that flexibility is exercised responsibly. While projects must adapt to evolving conditions, adaptation must occur within a disciplined risk-informed decision framework. This approach transforms scope control from a reactive administrative function into a proactive strategic safeguard.

Through structured reassessment of risk exposure, identification of new uncertainties, updating of mitigation strategies, and review of contingency reserves, the NCPBF project preserves execution stability, financial integrity, and security posture even when scope adjustments are necessary.

In summary, scope and risk are interdependent governance domains. Changes to one inevitably influence the other. By formally embedding risk reassessment within the scope control process, the project ensures that uncertainty is managed deliberately rather than discovered accidentally.

10. Scope & Benefits Integration:

The NCPBF project is not merely an infrastructure initiative; it is a strategic national capability investment designed to deliver measurable long-term benefits, including sovereign currency production capacity, enhanced monetary security, financial sustainability, operational resilience, and institutional strengthening. Therefore, scope definition and control must remain directly aligned with benefits realization objectives.

Scope & Benefits Integration ensures that every major deliverable within the project contributes meaningfully to defined strategic outcomes. Deliverables that do not support measurable benefits dilute focus, increase cost, introduce complexity, and potentially delay realization of intended value. Accordingly, disciplined alignment between scope components and benefits is essential.

Each major deliverable defined within the WBS must map to at least one defined benefit documented in the Benefits Management Plan. This traceability confirms that the deliverable exists for a justified strategic purpose. The mapping process ensures that infrastructure elements, technical systems, operational readiness initiatives, governance mechanisms, and compliance frameworks all contribute to specific value outcomes rather than existing as isolated technical outputs.

In addition to benefit alignment, each major deliverable must be linked to at least one measurable Key Performance Indicator (KPI). KPIs provide quantifiable evidence that the deliverable supports intended results. For example, installation of secure printing equipment may link to KPIs related to production capacity, error reduction rates, or quality consistency. Cybersecurity system deployment may align with KPIs measuring intrusion prevention effectiveness or system uptime resilience. Governance systems may align with audit compliance metrics or reporting accuracy standards.

This measurable linkage ensures that scope elements are not justified solely on conceptual value but demonstrate tangible performance contribution. KPI alignment also supports post-commissioning monitoring and ensures continuity between project outputs and operational performance measurement.

Furthermore, each major benefit must have an assigned Benefit Owner. The Benefit Owner is accountable for ensuring that deliverables translate into

sustained operational value after project completion. This reinforces the principle that projects deliver outputs, but operations realize benefits. By linking scope elements to accountable benefit ownership, the project prevents disconnect between construction completion and long-term institutional impact.

Scope elements that cannot be clearly mapped to defined benefits require executive-level justification prior to inclusion. This safeguard prevents unnecessary feature expansion, politically driven additions, or vendor-influenced enhancements that do not materially contribute to strategic objectives. Executive review ensures that scope remains disciplined and value-focused.

Integration between scope and benefits also strengthens decision-making during change control. When evaluating proposed scope modifications, decision-makers must assess not only cost and schedule impact, but also benefit alignment. A proposed change that increases cost but significantly enhances long-term benefit realization may warrant approval. Conversely, a change that adds technical complexity without measurable benefit contribution should be challenged or rejected.

The integration framework also supports prioritization. In situations where budget constraints or schedule pressures require scope reduction, benefit mapping helps determine which deliverables are essential and which may be deferred without compromising core value objectives.

Post-commissioning, this structured scope–benefit traceability facilitates performance monitoring. By linking deliverables to KPIs and benefit owners, the organization can measure whether the intended outcomes defined in the Business Case are being achieved. This reinforces accountability and strengthens institutional learning.

Ultimately, Scope & Benefits Integration ensures that the NCPBF project remains purpose-driven rather than output-driven. Deliverables exist not merely to complete construction, but to establish a secure, sustainable, and strategically aligned national capability.

By requiring that each major deliverable maps to defined benefits, measurable KPIs, and accountable benefit ownership, the project preserves value focus, protects investment logic, and ensures long-term sustainability.

11. Security & Confidentiality Controls:

The National Currency Printing and Secure Banknote Production Facility Project (NCPBF) operates within an environment of national-level security sensitivity. The nature of the project — involving secure printing technology, vault systems, cybersecurity infrastructure, regulatory controls, and institutional monetary integrity — requires that scope management incorporate strict security and confidentiality controls. Scope flexibility must never compromise national security posture, operational resilience, or regulatory compliance.

Security architecture scope elements are therefore subject to enhanced governance oversight. Any modification to components related to physical security, cybersecurity systems, surveillance infrastructure, secure printing mechanisms, vault construction, network architecture, or access control frameworks requires formal review and approval by the designated Security Board. These elements are classified as high-sensitivity deliverables and are excluded from standard operational change authorization thresholds. No scope adjustment affecting security-critical components may proceed without documented security impact assessment and explicit approval from authorized security governance authorities.

Access-controlled design components are subject to strict configuration management. All drawings, technical specifications, integration diagrams, and architectural documentation related to secure systems must be version-controlled, access-restricted, and maintained under secure document management protocols. Unauthorized duplication, distribution, or modification of such documentation is prohibited. Every revision must be traceable, formally approved, and archived in accordance with configuration control procedures.

Classified deliverables require restricted documentation handling procedures. These procedures include controlled storage, encrypted digital transmission where applicable, restricted access rights, role-based authorization controls, and documented audit trails. Distribution of classified scope documents must follow approved security protocols to prevent unauthorized disclosure or compromise. Physical documentation must be stored within secure environments, and digital access must be monitored through identity and access management controls.

Security review is integrated into the scope change process. Any proposed change affecting sensitive systems must undergo security risk assessment prior to governance review. This ensures that scope modifications do not inadvertently introduce vulnerabilities, weaken protective controls, or create exposure pathways within the facility's security architecture.

Unauthorized informal requests — whether originating from internal stakeholders, vendors, or external entities — are formally logged as governance exceptions. Informal scope modification attempts, particularly those affecting secure components, are treated as control violations and are documented for audit transparency. This ensures accountability and reinforces the principle that security-sensitive scope is governed through formal authority, not operational convenience.

The project adopts a "security-by-design and security-in-change" principle. Security controls are embedded within initial scope definition and remain active throughout the change control lifecycle. By integrating security governance into scope management, the NCPBF project preserves confidentiality, integrity, and availability of critical systems while maintaining compliance with national regulatory frameworks.

In summary, security and confidentiality controls are not supplementary safeguards; they are foundational elements of scope governance within the NCPBF project. Protection of classified deliverables, configuration control of sensitive components, and formal Security Board oversight ensure that scope flexibility never compromises national security objectives.

12. Scope Performance Monitoring:

Scope performance monitoring ensures that the approved Scope Baseline remains stable, measurable, and aligned with strategic objectives throughout execution. In accordance with PMI performance measurement principles, scope monitoring evaluates whether the project is delivering authorized work within approved boundaries and whether scope stability is being maintained.

Deliverable completion tracking is the primary mechanism for monitoring scope execution. Each work package defined within the WBS is tracked against its acceptance criteria, ensuring that deliverables are completed as defined in the Scope Baseline. Completion status is documented and validated through formal acceptance processes. Progress reporting is aligned with WBS control accounts to maintain structural clarity.

Earned Value correlation is used to monitor integration between scope, cost, and schedule performance. By linking scope completion to earned value metrics, the project evaluates whether work performed corresponds to approved deliverables and budget allocations. Variances between planned value, earned value, and actual cost may indicate scope execution inefficiencies, rework requirements, or emerging scope instability. This integrated monitoring supports early detection of deviation trends.

Change frequency analysis provides insight into scope stability. The project monitors the number, type, and magnitude of change requests over time. An increase in change frequency may signal unclear requirements, stakeholder misalignment, inadequate initial definition, or external pressure. By analyzing change patterns, governance bodies can proactively address root causes before instability escalates.

Trend analysis of change requests further strengthens monitoring discipline. The project evaluates whether changes are concentrated within particular deliverable streams, lifecycle phases, or technical domains. Persistent trends in specific areas may indicate design gaps, regulatory ambiguity, vendor integration challenges, or security architecture weaknesses. This analytical approach transforms change control data into strategic oversight intelligence.

Stage-gate compliance audits reinforce scope discipline at lifecycle transition points. Prior to moving from design to construction, procurement to installation, or integration to commissioning, formal audits confirm that scope for the preceding phase has been validated, accepted, and frozen. These audits ensure that no incomplete or undefined deliverables carry forward into subsequent phases.

Scope instability triggers governance review. Indicators of instability may include excessive change volume, repeated baseline adjustments, frequent rework, deviation from acceptance criteria, or inconsistent deliverable interpretation. When instability thresholds are exceeded, the issue is escalated to the appropriate governance body for corrective action planning. Corrective measures may include enhanced stakeholder alignment, scope clarification workshops, requirement re-baselining, or strengthened change control enforcement.

The objective of scope performance monitoring is not to eliminate change entirely, but to ensure that change occurs within disciplined boundaries and remains strategically justified. Stable scope contributes to predictable cost performance, controlled risk exposure, and successful benefit realization.

Through structured deliverable tracking, earned value integration, change trend analysis, and stage-gate audit discipline, the NCPBF project maintains continuous visibility over scope integrity and protects its baseline throughout the lifecycle.

13. Scope-Related Risks:

In large-scale, high-visibility national infrastructure projects such as the NCPBF initiative, scope-related risks represent one of the most significant threats to delivery stability. Scope instability can directly affect cost performance, schedule reliability, risk exposure, regulatory compliance, security integrity, and long-term benefit realization. Accordingly, scope-related risks are proactively identified, monitored, and mitigated as part of the integrated scope governance framework.

One of the most prominent risks is political intervention. Projects of national importance may attract external influence from institutional leaders, regulatory authorities, or government representatives seeking additional features, accelerated timelines, or expanded facility capabilities. While such requests may be strategically motivated, informal or late-stage political direction can undermine baseline stability and create cascading impacts across cost and schedule. To mitigate this risk, the project enforces strict governance thresholds and requires all scope modifications—regardless of origin—to follow the formal change control process. Strategic deviations require Executive Sponsor authorization, ensuring institutional accountability.

Scope creep through technical enhancement requests represents another common risk. Vendors, engineers, or internal specialists may propose technical improvements or advanced features during design or implementation phases. Although technically attractive, these enhancements may not align with approved objectives or financial assumptions. Without disciplined control, incremental enhancements can accumulate and materially alter project boundaries. Mitigation involves enforcing deliverable-based WBS discipline, requiring formal impact analysis, and ensuring all enhancements demonstrate measurable benefit contribution before approval.

Late-stage regulatory changes present additional scope risk. Adjustments to monetary regulations, compliance frameworks, security standards, or procurement rules may necessitate modifications to design or operational architecture. These changes may be mandatory and time-sensitive, increasing schedule and cost pressure. The project mitigates this exposure by maintaining continuous regulatory monitoring and incorporating compliance review

checkpoints within stage-gate governance processes. Early detection reduces disruptive late-stage modifications.

Vendor-driven specification expansion is another recognized risk in specialized infrastructure and technology projects. Equipment suppliers or system integrators may recommend upgrades, feature additions, or alternative configurations that exceed initial scope. While some recommendations may enhance performance, others may introduce unnecessary cost or complexity. Strict procurement specification control, configuration management discipline, and contractual scope boundaries mitigate this risk. Any vendor-proposed expansion must undergo formal change evaluation.

Stakeholder pressure for non-baselined features also poses risk. Operational teams, end users, or oversight bodies may request additional reporting capabilities, design alterations, or expanded functionality during implementation. While stakeholder engagement is essential, informal responsiveness can destabilize scope. Controlled stakeholder engagement mechanisms ensure that requests are documented, evaluated, and approved only if strategically justified.

Mitigation of scope-related risks relies on several governance mechanisms. Strict change thresholds ensure that minor adjustments do not escalate into uncontrolled expansion. Controlled stakeholder engagement prevents bypassing of formal approval pathways. A formal Requirements Traceability Matrix reinforces alignment between defined requirements, deliverables, and benefits, reducing ambiguity and preventing undocumented feature inclusion.

Through proactive identification and disciplined mitigation of scope-related risks, the NCPBF project preserves execution stability and protects baseline integrity throughout its lifecycle.

14. Scope Documentation Control:

Effective scope governance depends not only on structured definition and change control but also on disciplined documentation management. Scope documentation control ensures that approved scope information remains accurate, secure, accessible to authorized stakeholders, and protected from unauthorized alteration.

All scope documents—including the Scope Statement, WBS, WBS Dictionary, Change Register entries, validation records, and related configuration documentation—are subject to formal version control. Each document must include a version identifier, approval date, revision history, and authorizing authority. Version control ensures traceability of changes over time and supports audit transparency.

Scope documentation is stored within restricted-access repositories in accordance with the project's security and confidentiality controls. Access rights are assigned based on role-based authorization principles to ensure that only designated personnel may modify baseline documents. Read-only access may be granted to relevant stakeholders, but editing privileges remain tightly controlled.

Quarterly document review cycles are conducted to ensure that scope documentation remains current, accurate, and aligned with approved baselines. These reviews confirm that no undocumented modifications have occurred and that related documentation—such as cost baselines, schedules, and risk registers—remains synchronized with the Scope Baseline.

Updates to scope documentation may occur only through formal change control procedures. No manual adjustments, informal edits, or undocumented revisions are permitted. When a scope change is approved, corresponding updates to the Scope Statement, WBS, and WBS Dictionary must be executed under configuration management control and documented within revision history records.

Document retention policies ensure that historical baseline versions are archived for reference and audit purposes. This enables retrospective analysis of change patterns and governance effectiveness over time.

In addition to structural control, documentation integrity supports strategic alignment. Clear, current, and controlled scope documents reduce ambiguity, prevent misinterpretation, and strengthen stakeholder confidence in governance processes.

Through disciplined version control, restricted access management, scheduled review cycles, and strict change authorization requirements, the NCPBF project ensures that scope documentation remains a reliable and authoritative reference throughout execution and transition to operations.

15. Roles & Responsibilities:

Role	Responsibility
Project Manager	Scope integrity enforcement
PMO	Governance oversight
Change Control Board	Scope decision authority
Security Board	Security-related scope approval
Sponsor	Strategic scope decisions
Work Package Owners	Deliverable accountability

16. Scope Management Success Criteria:

The effectiveness of the Scope Management System within the NCPBF Project is measured not merely by the existence of documented processes, but by demonstrable performance outcomes that reflect disciplined control, strategic alignment, and execution stability. Scope management success is evaluated through structured performance indicators that confirm the integrity of the Scope Baseline throughout the project lifecycle.

One key success indicator is that change frequency remains within predefined governance thresholds. While controlled change is expected in complex projects, excessive or uncontrolled change signals weak initial definition, stakeholder misalignment, or governance gaps. The project monitors the volume, magnitude, and pattern of approved and rejected change requests. A stable and predictable change trend indicates that scope definition was sufficiently robust and that governance discipline is functioning effectively.

Another critical success criterion is the absence of unauthorized scope additions. All deliverables executed within the project must be represented within the approved Scope Baseline and WBS structure. Work performed outside authorized boundaries constitutes a governance violation and reflects breakdown in control systems. A successful scope management system ensures that no work is initiated without formal approval and that configuration management controls prevent undocumented expansion.

Traceability between deliverables and approved benefits represents another core measure of success. Every major deliverable must be linked to defined benefits and measurable KPIs as outlined in the Benefits Management Plan. If deliverables cannot be clearly mapped to strategic outcomes, scope discipline has weakened. A successful system ensures that scope remains purpose-driven and aligned with value realization objectives rather than drifting toward technical or stakeholder-driven enhancements lacking measurable impact.

Respect for stage-gate scope freezes is another important success indicator. Phase transitions—such as moving from design to construction, procurement to installation, or integration to commissioning—must occur only after formal validation and scope freeze confirmation. If downstream phases begin while upstream scope remains unstable or undefined, the risk of rework and cost

escalation increases. Successful scope management ensures that stage-gate approvals are consistently honored and documented.

Protection of security-related scope elements is also a defining success measure. Security architecture, cybersecurity systems, controlled access infrastructure, and classified design components must remain stable unless formally reviewed and approved by authorized governance bodies. Unauthorized modification of security scope represents a critical failure of governance. A successful system ensures that security-sensitive components remain protected under enhanced oversight and configuration control.

Another essential success indicator is that commissioning occurs without rework attributable to uncontrolled scope change. If deliverables require redesign, reconstruction, or reinstallation due to late-stage scope alterations, this indicates inadequate scope control. A mature scope management system minimizes rework by enforcing disciplined change control, structured validation, and timely freeze mechanisms.

In addition to these indicators, qualitative measures support evaluation of scope management maturity. These include clarity of documentation, stakeholder confidence in scope governance processes, audit transparency, and alignment between scope, cost, schedule, and risk baselines.

Collectively, these criteria demonstrate whether the Scope Management Plan has functioned as an active governance safeguard rather than a passive administrative document. Success is achieved when scope remains stable, aligned, traceable, and controlled—allowing the NCPBF project to deliver authorized capability within approved boundaries while preserving financial discipline, regulatory compliance, security integrity, and long-term benefit realization.

A stable scope environment is the foundation of predictable performance. Predictable performance is the foundation of strategic success.

Approval:

Role	Name	Signature	Date
Project Sponsor	Mr. Ahmad Khan		
Project Manager	Mr. Reshtin, PMP®		
PMO Representative			